Cover Page

April 25, 1998

Cathy Kemelmacher
Production Editor
IEEE Communications Society
345 East 47th Street
New York, NY 10017 USA
tel: +1-212-705-7854
fax: +1-212-705-7865

Dear Ms. Kemelmacher:

Please find enclosed our submission of a paper for IEEE Communications Letters including disk and copyright release.

I work in a windows environment so cannot submit electronically what was recommended. If you can use them, I have included a disk with the text in RTF format and the figures in MS Powerpoint.

Sincerely,

Steve F. Russell, Ph.D., P.E.
Associate Professor
Electrical Engineering
333 Coover E CPE
Iowa State University
Ames, Iowa 50011

Tel: 515-294-1273
Fax; 515-294-8432
Email: sfr@iastate.edu
http://www.public.iastate.edu/~sfr/homepage.html

cc: jourlet7.wpd

Security Considerations for Future Wireless Standards

Steve F. Russell, *Senior Member,* and Michael L. Hageman, *Student Member, IEEE*

***Abstract*- Security considerations are gaining increasing importance as the general public increases their use of Personal Communication Services (PCS) and other wireless technology such as cordless phones, pagers, and wireless modems. The need to enhance robustness and security in wireless applications is very apparent. We have looked at new wireless systems to assess their current security strengths and weakness with our focus being the IS-95A CDMA standard, in particular, the air interface between the mobile and the base station. This paper is an introduction to our research approach and current results.**

***Index Terms*- Security, CDMA, Cellular Fraud, IS-95A, wireless standards.**

I. INTRODUCTION

How many of us take for granted the security of modern telecommunications technology? It is well publicized that older wireline and wireless analog systems have few security features. For AMPS cellular, fraud by number cloning has been highly publicized. The technology for AMPS number cloning is inexpensive and readily available. The newer digital cellular standards, such as the IS-95A CDMA [1], have incorporated several new security features that are major improvements over AMPS. For example, IS-95A makes number cloning very difficult, however eaves-dropping is still possible because of deficiencies in the standard. It is apparent that modifications are needed to improve security without obsoleting current phones. In this paper, we will present our view of telecommunications security and illustrate examples of some weaknesses in IS-95A with suggested ways to overcome them.

It is important to communicate the motivation for this research. The 1994 NSF Airlie House [2] workshop on *Research Priorities in Networking and Communications* reported that networks and communications still remain vulnerable to malicious attacks and advised that a "coherent security architecture is needed." The 1997 NSF Airlie House report [3] on *Research Priorities in Wireless and Mobile Communications and Networks* listed the important security issues as authentication, encryption, anonymity, and intrusion detection.

The theme for Milcom 97, *Integrating Military and Commercial Communications for the Next Century*, provided a forum for exchanging ideas about the latest technologies in both commercial (COTS) and military communication systems. It was apparent at the conference that more robustness and security would be needed in commercial

telecommunication systems.

In general, security for commercial systems has been focused on the issues most pertinent to the service and infrastructure providers - number cloning and new service fraud. This research covers a broader scope of security by also including issues important to subscribers, for example, denial of service, eavesdropping, and spoofing.

Our goal is to develop enhancements to the standards that overcome security weaknesses, not to give aid to those attempting to invade the privacy of the cellular subscriber, nor do we mean to criticize the TIA/EIA IS-95-A standard. The approach here is similar to that followed by the computer industry, which generally publicizes known security breaches so that system administrators can take corrective measures. So far, wireless systems have benefited from a level of complexity that makes “hacking” impractical and expensive but criminals are becoming more sophisticated.

We envision three levels of security and robustness for the future global telecommunications infrastructure:

Level-1 Unsecured Commercial - Users not needing sophisticated security.

Level-2 Secured Commercial - Federal and State governments, financial institutions, corporate businesses, and other users wanting additional security and privacy.

Level-3 Secured Military.

Our research will focus on Level-2 security which we define as an enhanced wireless service closely coupled with existing wireless services. Our security model classifies attacks into the areas given in Fig. 1 which is a modification of the military model [4]. The success of future wireless systems depends a great deal on the effective use of sophisticated radio communication design.

Historically, military attacks have employed *electronic countermeasures* (ECM) to *detect* the presence of wireless signals and either *disrupt* them or *exploit* them. Military wireless systems can be disrupted by *jamming* or *by locating and destroying* them. On the other hand, *exploitation* involves using the transmissions for intelligence and counter-intelligence purposes. Prior to the development of high quality data security and transmission security techniques, it was possible to gather intelligence from the received signals by *demodulating* and *decoding* (deciphering) them. For simple systems it is also possible to "spoof" (or mimic) them to provide false information (counter-intelligence). Radio transmissions can also be exploited, even when they employ high quality security techniques, by simple *radio*

location methods to implement *position monitoring*

Electronic counter-countermeasures (ECCM) must be employed in public systems to minimize the impact of increasingly sophisticated ECM (such as jammers and counterfeit bases) and must become a key part of Level-2 security system design. ECCM techniques may be classified as *anti-intercept* (AI), *anti-jam* (AJ), or *data security*. Anti-intercept techniques (called Low Probability of Intercept, LPI) try to prevent the attacker from detecting and locating the source of radio transmissions. If successful, AI obviates the need for AJ or data security. When the system AI features have been overcome and the signal detected, the attacker may choose to either exploit or disrupt. In most cases, the system will have data (cryptographic) security to prevent decoding or spoofing.

The communication security issues in commercial systems differ with military objectives in some aspects. For example, it is not practical to secure commercial systems against locate & destroy attacks. Also, detection is not an issue since existing commercial wireless signals are easily detected. This leaves us with the security issues outlined in Fig. 1.

II. COMMERCIAL SECURITY ISSUES

The following is a brief description of each of the issues for commercial systems. The examples given are taken from our work with IS-95A CDMA and AMPS.

Counterfeit Communication

Our example of counterfeit communications derives from the use of a counterfeit base station to spoof the user into thinking that an authenticated transaction has taken place. The example we will use comes from the recent movie “The Game” [5] where the main character makes a wireless telephone call to his Swiss bank to inquire about his account balance. The character begins to believe that the call was actually placed to a counterfeit base station and that he has divulged his account information to an unknown party.

Position Monitoring

Position determination by time-delay or angle-of-arrival methods is possible with all wireless systems including AMPS and IS-95A CDMA. Federally mandated position location for E911 emergency services means

that all PCS providers will have this function implemented and available within the wireless network. Users will need to demand that the implementation allow them to authorized or deny this function at their discretion. An attacker can also use the same technology to locate a user.

Eavesdropping (3rd Party)

Currently, the only services where eavesdropping is a major issue are AMPS and paging. In AMPS, a simple “scanner” receiver can listen in because AMPS uses channelized wideband FM modulation. In pagers, it is a matter of decoding the digital phone number, address, or message. Eavesdropping technology is not yet readily available for IS-95A or similar digital services but technology advances will inevitably make it possible. There is also a federal mandate for court-ordered eavesdropping by local law enforcement which means that this function will be implemented and available within the wireless network.

Denial of Service (User)

Base station impersonation can also lead to denial of service. The simplest example is for the counterfeit base to deny authentication for the mobile whereby the mobile user believes that the mobile or the base is defective. The other, more obvious, method is radio jamming of the spectrum used for the communication. Jamming is very effective against IS-95A CDMA since a moderately powered, single-frequency jammer can block the mobile station from all cell sites.

Theft of Services

Number cloning and new service fraud and the major problems currently facing service providers. Digital services will greatly reduce number cloning until attacker technology “catches up.” Our research does not address new service fraud.

Denial of Service (Base)

Simple jamming can also bring down one or more IS-95A cell sites. Surprisingly, jamming is less effective

against AMPS since a strong broadband jammer is required. Intelligent broadband jamming can cause the base station to reduce its radius of coverage to the point where only a few of the closest users can obtain service.

III. IS-95A EXAMPLE

In order to make more clear some of the issues of cellular security, an example of eavesdropping by an unauthorized third party (transgressor) will be given. As background for the scenario, assume first that the IS-95A cellular user is in the middle of a sensitive conversation on her phone in the vicinity of the transgressor. The transgressor first jams (**Denial of Service**) the cellular user. The phone, now being disconnected from the authentic base station, attempts to find another base station. The transgressor has a counterfeit base station up and running with a very strong signal. The cellular user's phone detects this strong signal and establishes a link (**Counterfeit Communication**). When the cellular user calls the second party to continue the conversation, the call is placed through the transgressor, giving the transgressor the ability to listen in on both sides of the conversation (**Eavesdropping**), as shown in Figure 2. One may believe that, because the IS-95A system has the ability to scramble and/or encrypt the voice channel, that the transgressor would be unable to decipher (hear) the conversation. This would be true except in the IS-95A system, encryption of voice data is determined by the base station and not the mobile station. Therefore, the counterfeit base station simply denies encryption for the mobile under attack.

IV. CONCLUSION

This paper was intended to give only a very brief look at the most important issues in airlink security for wireless networks. We see a great need for intensive research in this area and have provided some examples for thought. The research program at Iowa State is also looking at the Mobile Switching Center and its interactions with the base station and the public network. The authors are submitting a paper to the IEEE Transactions on Communications that discusses the details of the airlink security issues in IS-95A.

REFERENCES

[1] Telecommunications Industry Association, TIA/EIA IS-95A, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System," May 1995.

[2] "Research Priorities in Networking and Communications," Report to the NSF Division of Networking and Communications Research and Infrastructure by Members of the Workshop Held May 12-14, 1994, Airlie House, Virginia. http://www.cise.nsf.gov/ncri/arliehou.txt

[3] NSF workshop, "Research Priorities in Wireless and Mobile Communications and Networks - Summary," Airlie House Virginia, March 24-26, 1997. http://www.cise.nsf.gov/ncri/wirelswkshp.html

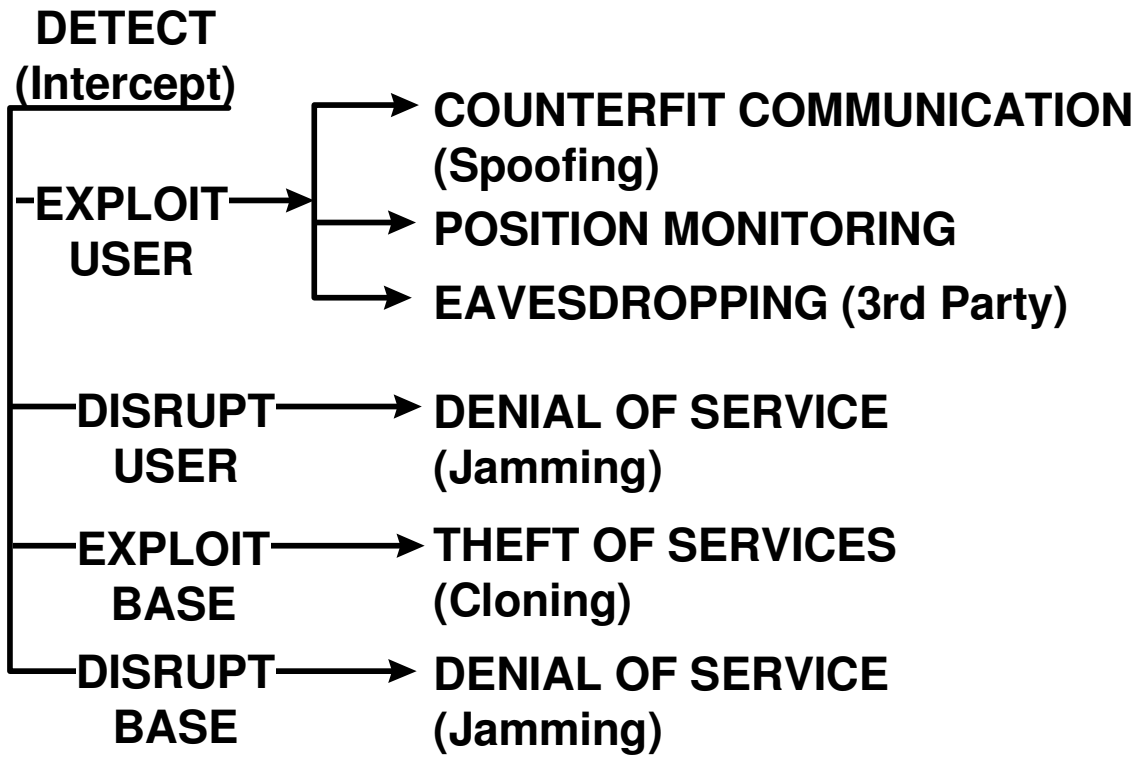
[4] ***Anti-jam Techniques for Communication and Navigation Systems***, Rockwell International, Collins Avionics & Missiles Group, Advanced Technology and Engineering, 28 September 1979.

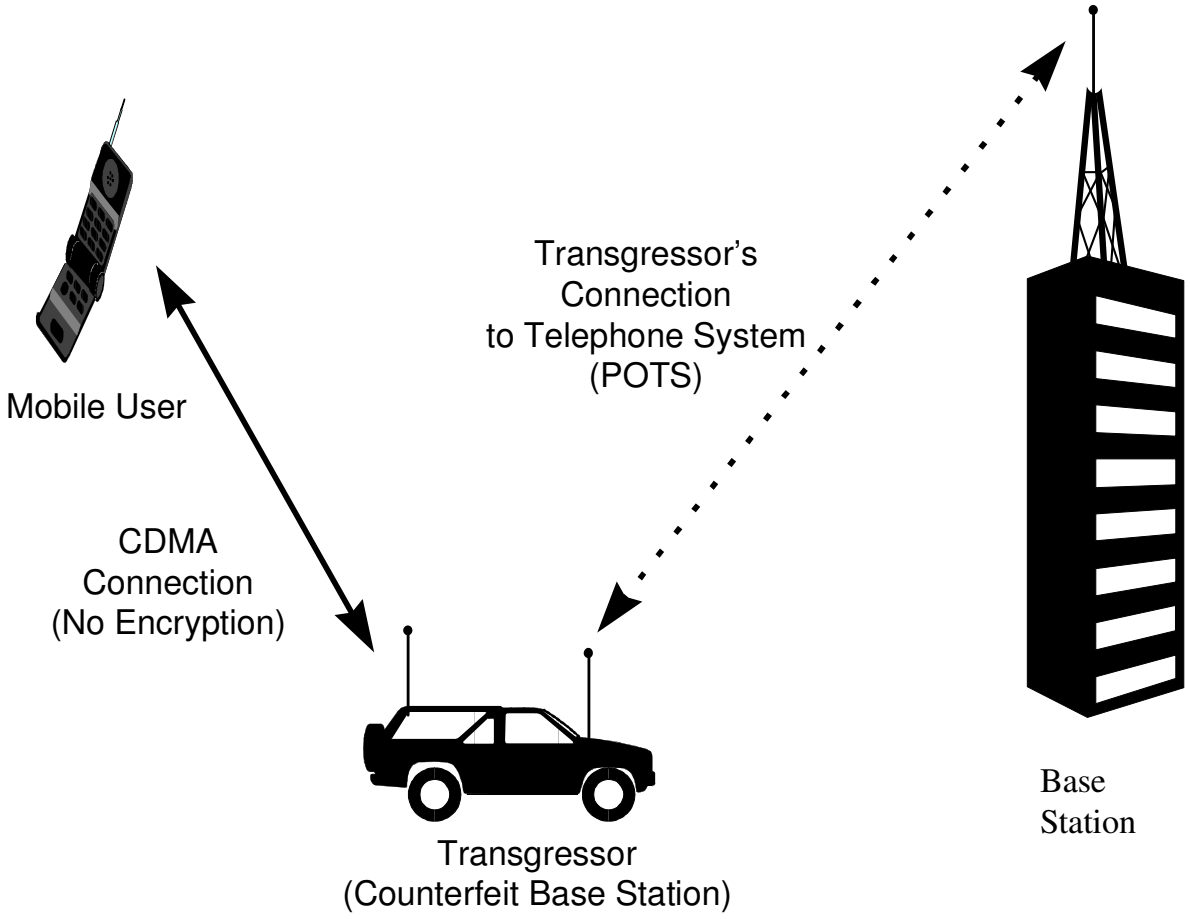
[5] *The Game*, staring Michael Douglass, PolyGram, 1997.

FIGURE CAPTIONS

Figure 1. Communication System Security Overview for Commercial Systems

Figure 2. Using a Counterfeit Base Station (Transgressor) to establish a two way link in the CDMA environment.


DETECT
(Intercept)
EXPLOIT
USER
COUNTERFIT COMMUNICATION
(Spoofing)
POSITION MONITORING
EAVESDROPPING (3rd Party)
DISRUPT
USER
DENIAL OF SERVICE
(Jamming)
EXPLOIT
BASE
THEFT OF SERVICES
(Cloning)
DISRUPT
BASE
DENIAL OF SERVICE
(Jamming)


Transgressor's
Connection
to Telephone System
(POTS)
Mobile User
CDMA
Connection
(No Encryption)
Base
Station
Transgressor
(Counterfeit Base Station)

Security Considerations for Future Wireless Standards

Steve F. Russell, *Senior Member,* and Michael L. Hageman, *Student Member, IEEE*

***Abstract*- Security considerations are gaining increasing importance as the general public increases their use of Personal Communication Services (PCS) and other wireless technology such as cordless phones, pagers, and wireless modems. The need to enhance robustness and security in wireless applications is very apparent. We have looked at new wireless systems to assess their current security strengths and weakness with our focus being the IS-95A CDMA standard, in particular, the air interface between the mobile and the base station. This paper is an introduction to our research approach and current results.**

***Index Terms*- Security, CDMA, Cellular Fraud, IS-95A, wireless standards.**

I. INTRODUCTION

How many of us take for granted the security of modern telecommunications technology? It is well publicized that older wireline and wireless analog systems have few security features. For AMPS cellular, fraud by number cloning has been highly publicized. The technology for AMPS number cloning is inexpensive and readily available. The newer digital cellular standards, such as the IS-95A CDMA [1], have incorporated several new security features that are major improvements over AMPS. For example, IS-95A makes number cloning very difficult, however eaves-dropping is still possible because of deficiencies in the standard. It is apparent that modifications are needed to improve security without obsoleting current phones. In this paper, we will present our view of telecommunications security and illustrate examples of some weaknesses in IS-95A with suggested ways to overcome them.

It is important to communicate the motivation for this research. The 1994 NSF Airlie House [2] workshop on *Research Priorities in Networking and Communications* reported that networks and communications still remain vulnerable to malicious attacks and advised that a "coherent security architecture is needed." The 1997 NSF Airlie House report [3] on *Research Priorities in Wireless and Mobile Communications and Networks* listed the important security issues as authentication, encryption, anonymity, and intrusion detection.

The theme for Milcom 97, *Integrating Military and Commercial Communications for the Next Century*, provided a forum for exchanging ideas about the latest technologies in both commercial (COTS) and military communication systems. It was apparent at the conference that more robustness and security would be needed in commercial telecommunication systems.

In general, security for commercial systems has been focused on the issues most pertinent to the service and infrastructure providers - number cloning and new service fraud. This research covers a broader scope of security by also including issues important to subscribers, for example, denial of service, eavesdropping, and spoofing.

Our goal is to develop enhancements to the standards that overcome security weaknesses, not to give aid to those attempting to invade the privacy of the cellular subscriber, nor do we mean to criticize the TIA/EIA IS-95-A standard. The approach here is similar to that followed by the computer industry, which generally publicizes known security breaches so that system administrators can take corrective measures. So far, wireless systems have benefited from a level of complexity that makes “hacking” impractical and expensive but criminals are becoming more sophisticated.

We envision three levels of security and robustness for the future global telecommunications infrastructure:

Level-1 Unsecured Commercial - Users not needing sophisticated security.

Level-2 Secured Commercial - Federal and State governments, financial institutions, corporate businesses, and other users wanting additional security and privacy.

Level-3 Secured Military.

Our research will focus on Level-2 security which we define as an enhanced wireless service closely coupled with existing wireless services. Our security model classifies attacks into the areas given in Fig. 1 which is a modification of the military model [4]. The success of future wireless systems depends a great deal on the effective use of sophisticated radio communication design.

Historically, military attacks have employed *electronic countermeasures* (ECM) to *detect* the presence of wireless signals and either *disrupt* them or *exploit* them. Military wireless systems can be disrupted by *jamming* or *by locating and destroying* them. On the other hand, *exploitation* involves using the transmissions for intelligence and counter-intelligence purposes. Prior to the development of high quality data security and transmission security techniques, it was possible to gather intelligence

November 20, 1997 Initial Draft April 25, 1998 Submitted Draft

from the received signals by *demodulating* and *decoding* (deciphering) them. For simple systems it is also possible to "spoof" (or mimic) them to provide false information (counter-intelligence). Radio transmissions can also be exploited, even when they employ high quality security techniques, by simple *radio location* methods to implement *position monitoring*

Electronic counter-countermeasures (ECCM) must be employed in public systems to minimize the impact of increasingly sophisticated ECM (such as jammers and counterfeit bases) and must become a key part of Level-2 security system design. ECCM techniques may be classified as *anti-intercept* (AI), *anti-jam* (AJ), or *data security*. Anti-intercept techniques (called Low Probability of Intercept, LPI) try to prevent the attacker from detecting and locating the source of radio transmissions. If successful, AI obviates the need for AJ or data security. When the system AI features have been overcome and the signal detected, the attacker may choose to either exploit or disrupt. In most cases, the system will have data (cryptographic) security to prevent decoding or spoofing.

The communication security issues in commercial systems differ with military objectives in some aspects. For example, it is not practical to secure commercial systems against locate & destroy attacks. Also, detection is not an issue since existing commercial wireless signals are easily detected. This leaves us with the security issues outlined in Fig. 1.

II. COMMERCIAL SECURITY ISSUES

The following is a brief description of each of the issues for commercial systems. The examples given are taken from our work with IS-95A CDMA and AMPS.

Counterfeit Communication

Our example of counterfeit communications derives from the use of a counterfeit base station to spoof the user into thinking that an authenticated transaction has taken place. The example we will use comes from the recent movie “The Game” [5] where the main character makes a wireless telephone call to his Swiss bank to inquire about his account balance. The character begins to believe that the call was actually placed to a counterfeit base station and that he has divulged his account information to an unknown party.

Position Monitoring

Position determination by time-delay or angle-of-arrival methods is possible with all wireless systems including AMPS and IS-95A CDMA. Federally mandated position location for E911 emergency services means that all PCS providers will have this function implemented and available within the wireless network. Users will need to demand that the implementation allow them to authorized or deny this function at their discretion. An attacker can also use the same technology to locate a user.

Eavesdropping (3rd Party)

Currently, the only services where eavesdropping is a major issue are AMPS and paging. In AMPS, a simple “scanner” receiver can listen in because AMPS uses channelized wideband FM modulation. In pagers, it is a matter of decoding the digital phone number, address, or message. Eavesdropping technology is not yet readily available for IS-95A or similar digital services but technology advances will inevitably make it possible. There is also a federal mandate for court-ordered eavesdropping by local law enforcement which means that this function will be implemented and available within the wireless network.

Denial of Service (User)

Base station impersonation can also lead to denial of service. The simplest example is for the counterfeit base to deny authentication for the mobile whereby the mobile user believes that the mobile or the base is defective. The other, more obvious, method is radio jamming of the spectrum used for the communication. Jamming is very effective against IS-95A CDMA since a moderately powered, single-frequency jammer can block the mobile station from all cell sites.

Theft of Services

Number cloning and new service fraud and the major problems currently facing service providers. Digital services will greatly reduce number cloning until attacker technology “catches up.” Our research does not address new service fraud.

Denial of Service (Base)

Simple jamming can also bring down one or more IS-95A cell sites. Surprisingly, jamming is less effective against AMPS since a strong broadband jammer is required. Intelligent broadband jamming can cause the base station to reduce its radius of coverage to the point where only a few of the closest users can obtain service.

III. IS-95A EXAMPLE

In order to make more clear some of the issues of cellular security, an example of eavesdropping by an unauthorized third party (transgressor) will be given. As background for the scenario, assume first that the IS-95A cellular user is in the middle of a sensitive conversation on her phone in the vicinity of the transgressor. The transgressor first jams (**Denial of Service**) the cellular user. The phone, now being disconnected from the authentic base station, attempts to find another base station. The transgressor has a counterfeit base station up and running

with a very strong signal. The cellular user's phone detects this strong signal and establishes a link (**Counterfeit Communication**). When the cellular user calls the second party to continue the conversation, the call is placed through the transgressor, giving the transgressor the ability to listen in on both sides of the conversation (**Eavesdropping**), as shown in Figure 2. One may believe that, because the IS-95A system has the ability to scramble and/or encrypt the voice channel, that the transgressor would be unable to decipher (hear) the conversation. This would be true except in the IS-95A system, encryption of voice data is determined by the base station and not the mobile station. Therefore, the counterfeit base station simply denies encryption for the mobile under attack.

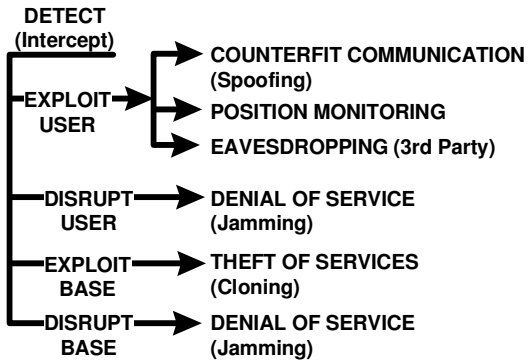


Figure 1. Communication System Security Overview for Commercial Systems

IV. CONCLUSION

This paper was intended to give only a very brief look at the most important issues in airlink security for wireless networks. We see a great need for intensive research in this area and have provided some examples for thought. The research program at Iowa State is also looking at the Mobile Switching Center and its interactions with the base station and the public network. The authors are submitting a paper to the IEEE Transactions on Communications that discusses the details of the airlink security issues in IS-95A.

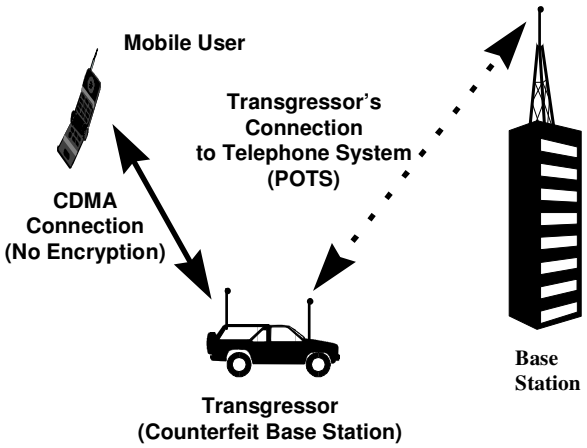


Figure 2. Using a Counterfeit Base Station (Transgressor) to establish a two way link in the CDMA environment.

REFERENCES

[1] Telecommunications Industry Association, TIA/EIA IS-95A, "Mobile Station-Base Station Compatibility Standard for Dual-Mode Wideband Spread Spectrum Cellular System," May 1995.

[2] "Research Priorities in Networking and Communications," Report to the NSF Division of Networking and Communications Research and Infrastructure by Members of the Workshop Held May 12-14, 1994, Airlie House, Virginia. http://www.cise.nsf.gov/ncri/arliehou.txt

[3] NSF workshop, "Research Priorities in Wireless and Mobile Communications and Networks - Summary," Airlie House Virginia, March 24-26, 1997. http://www.cise.nsf.gov/ncri/wirelswkshp.html

[4] ***Anti-jam Techniques for Communication and Navigation Systems***, Rockwell International, Collins Avionics & Missiles Group, Advanced Technology and Engineering, 28 September 1979.

[5] *The Game*, staring Michael Douglass, PolyGram, 1997.

View publication stats